

**IT IS SO ORDERED.**

/s/ Solomon Oliver, Jr.

IN THE UNITED STATES DISTRICT COURT     United States District Judge  
FOR THE NORTHERN DISTRICT OF OHIO     3/30/2021  
EASTERN DIVISION

ALBERT PICKETT, JR., KEYONNA	)	CASE NO. 1:19-cv-02911-SO
JOHNSON, JAROME MONTGOMERY,	)	
ODESSA PARKS, and TINIYA SHEPHERD	)	JUDGE SOLOMON OLIVER, JR.
(f/k/a/ TINIYA HALL), on behalf of	)	
themselves and all others similarly situated,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	
	)	<b><u>STIPULATION REGARDING</u></b>
CITY OF CLEVELAND,	)	<b><u>ELECTRONICALLY STORED</u></b>
	)	<b><u>INFORMATION AND HARD COPY</u></b>
Defendant.	)	<b><u>PROTOCOL</u></b>
	)	

Plaintiffs Albert Pickett, Jr., Keyonna Johnson, Jarome Montgomery, Odessa Parks, and Tiniya Shepherd and Defendant the City of Cleveland (collectively, the “Parties”) agree to the following protocol for production of electronically stored information (“ESI”) and paper (“hardcopy”) documents. Subject to any protective order that may be entered in this action, this protocol governs all production in the matter. This protocol has the objective to facilitate the just, speedy, and cost-proportionate completion of discovery of ESI and hardcopy documents and to promote, whenever possible, the early resolution of disputes regarding discovery without Court intervention, including disputes pertaining to scope or costs. Nothing in this protocol shall limit a party’s right to seek or object to discovery as set out in applicable rules, to rely on any protective order entered in this action concerning protection of confidential or otherwise sensitive information, or to object to the authenticity or admissibility of any hardcopy document or ESI produced in accordance with this protocol. The mere production of ESI as part of a mass production shall not itself constitute a waiver for any purpose.

## **I. GENERAL AGREEMENTS**

### **A. *Ongoing Cooperation among the Parties.***

The parties are aware of the importance the Court places on cooperation and commit to continue to consult and cooperate reasonably as discovery proceeds.

### **B. *Proportionality.***

1. Reasonable Discovery Limits. The proportionality standard set forth in Federal Rule of Civil Procedure 26(b)(1) (“Rule”) shall apply to discovery in this action. Consistent with that proportionality standard, the Parties agree to cooperate in identifying appropriate limits on discovery, including phased discovery and limits on the number of custodians, on discoverable data sources, on the relevant period, and on the permissible scope of requests for production. Requests for production of ESI, shall be reasonably targeted, clear, and as specific as possible, rather than general discovery of a product or business.

2. Discoverable Custodians and Non-Custodial Data Sources. Consistent with the proportionality standard, within a reasonable time after propounding of document requests and the entry of this protocol by the court, each Party shall provide to the other Party up to ten (10) of the Party’s Key Custodians, as well as a list of non-custodial data repositories, whose reasonably accessible ESI will be searched for relevant and proportional information. Custodians shall be identified by name, current or last-known title, and a brief description of current or last-known employment duties. Should the Parties, through the discovery process, identify a legitimate need to conduct additional reasonable and proportional discovery related to new Key Custodians or non-custodial data sources, the Parties shall meet and confer on additional discovery, or if the Parties cannot agree, may seek the assistance of the Court.

3. Discovery Concerning Preservation and Collection Efforts. Discovery concerning the preservation and collection efforts of another party can contribute to unnecessary expense and delay and may inappropriately implicate work product and attorney-client privileged matter. If there is a reasonable dispute concerning the scope of a party’s preservation

or collection efforts, before discovery about such efforts is initiated, the parties or their counsel shall meet and confer to address the specific stated need for such discovery, its relevance to claims and defenses, its proportionality to the needs of the case, and the availability and suitability of alternative, less burdensome means to obtain the information.

4. On-Site Inspections of ESI. On-site inspections of ESI under Rule 34(b) shall be permitted, if at all, only upon a good-faith showing by the Requesting Party of good cause and specific need or upon agreement of the parties. As appropriate, the Court may condition on-site inspections of ESI, as authorized in the preceding sentence, to be performed by independent third-party experts.

5. Non-Discoverable ESI. Consistent with the proportionality standard, and absent a Party's specific written notice for good cause, the following categories of ESI are presumed to be inaccessible and not discoverable:

- (a) ESI deleted in the normal course of business before the time a preservation obligation in this matter came into effect;
- (b) Backup data files that are maintained in the normal course of business for purposes of disaster recovery, including (but not limited to) backup tapes, disks, SAN, and other forms of media, and that are substantially duplicative of data more accessible elsewhere;
- (c) Deleted, "slack," fragmented, or unallocated data only accessible by forensics;
- (d) Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system;
- (e) On-line access data such as (without limitation) temporary internet files, history files, cache files, and cookies;

- (f) The metadata fields relating to when a document was last-opened or last-printed;
- (g) Electronic data (*e.g.*, call logs, email, calendars, contact data, notes, *etc.*) sent to or from mobile devices (*e.g.*, iPhone, iPad, Android, and Blackberry devices) provided that a copy of all such electronic data is saved elsewhere (such as on a server, laptop, desktop computer or cloud storage);
- (h) Server, system, network, or software application logs;
- (i) Data remaining from systems no longer in use that is unintelligible on the systems in use;
- (j) Electronic data temporarily stored by laboratory equipment or attached electronic equipment, provided that such data is not ordinarily preserved as part of a laboratory report;
- (k) Software files included on the National Institute of Standards and Technology (NIST) Modern RDS (minimal) list obtained from <https://www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl/nsrl-download/current-rds>;
- (l) Structural files not material to individual file contents (*e.g.*, .CSS, .XSL, .XML, .DTD, *etc.*);
- (m) Operating System files that do not store user-created content (*e.g.*, CAT, DLL, DMP, EXE, FON, PNF, OPS, SYS, *etc.*);
- (n) Application source code, configuration, and other similar files necessary for the function of an application that do not store user-created content during ordinary use (*e.g.* BAK, BIN, CFG, DBF, DAT, JS, JSON, JAR, LUA, MSB, RES, WINNT, YTR, *etc.*). Note that this does not

include relevant structured data that may use one of the preceding file extensions (*e.g.*, DAT).

**6. Disaster-Recovery Backup Data.** Consistent with the proportionality standard, and absent a Party's specific written notice for good cause, no Party shall be required to modify or suspend procedures, including rotation of backup media, used in the normal course of business to back up data and systems for disaster recovery purposes. Absent a showing of good cause, such backup media shall be considered to be not reasonably accessible.

**C. *No Designation of Discovery Requests.***

**1.** Productions of hardcopy documents and ESI in the reasonably usable form set out in this protocol, including Attachment A, need not be organized and labeled to correspond to the categories in the requests. The Parties will meet and confer on the potential identification of any reasonable requests for groups of Documents by Bates number responsive to specific discovery requests.

**D. *Redactions.***

**1.** The Producing Party may redact from any Group IV TIFF image ("TIFF"), metadata field, or native file, material: (1) that is protected from disclosure by applicable privilege or immunity, (2) governed by applicable privacy law or regulation, or (3) that is non-responsive. Redactions shall be clearly marked on the face of the document in the redaction field as "Redacted for Privilege" for privilege and confidential redactions, "Redacted as Non-Responsive" for non-responsive redactions and "Redacted for Privacy" for redactions governed by applicable privacy law or regulation, including personal identifying information. Documents redacted for any reason do not need to be placed on a redaction or privilege log as long as the reasons for the redaction is clearly marked on the face of the redaction itself (*e.g.* Redacted for Privacy, Redacted as Privileged, Redacted as Non-Responsive, etc.) and the REDACTED and REDACTED TYPE metadata fields for the redacted documents are provided as set forth in Attachment A. In preparing document families for production, the Producing Party

may also redact entire attachments that are wholly non-responsive and/or may produce slipsheets in their place that identify the document is withheld as non-responsive. The Parties will meet and confer on any redactions that a Party feels, in good faith, does not provide sufficient context to the responsive portions of the redacted document.

2. As is sometimes the case, Excel documents, for example, when imaged in TIFF form, result in an inordinate amount of pages that do not substantially resemble the native Excel document. Should the Parties find this to be the case with any Excel documents needing redaction, the Producing Party may produce the document in “modified native” format. Under “modified native” format, the Producing Party would delete the redactable information and replace it with the proper redaction nomenclature above and the words “by Counsel” (*e.g.*, “Redacted for Privilege by Counsel”). The “modified native” document would be produced with the metadata for the original document. For any document produced in this fashion, the Producing Party must preserve a pristine copy of the original document.

3. The Parties recognize that other documents, when imaged in TIFF form, will be rendered unusable or unintelligible. In those instances, the Parties will meet and confer concerning reproduction in a “modified native” format, or other manner to address the issue with the TIFF version of the document.

## **II. ELECTRONICALLY STORED INFORMATION.**

### **A. *Production in Reasonably Usable Form.***

1. The parties shall produce electronically stored information in reasonably usable form. Except as stated in paragraphs II.B and II.C below, or as agreed hereafter by the parties, such reasonably usable form shall be the single-page black and white TIFF images at 300 DPI, Group IV compression with extracted or OCR text and associated metadata as set out in Attachment A, which is incorporated in full in this protocol (“TIFF format”). If the Receiving Party, for good cause explained in the request and subject to the proportionality standard, seeks production in native format of specifically identified ESI produced originally in TIFF format, the

Producing Party shall respond reasonably and in good faith to any such request. Procedures for production of a native file in response to any such request are set out in Attachment A, Paragraph A.13.b.

2. Each Party may make requests, for good cause and subject to the proportionality standard, for production of specifically identified documents in color.

3. In the event that electronically stored information discoverable in this proceeding was previously produced in another legal proceeding, the Producing Party may request to produce that information to the Receiving Party in the form in which it was previously produced. The Parties shall meet and confer about any good faith concerns of the Producing Party related to producing such information according to the specifications contained in this protocol, and the Parties will negotiate in good faith to reach a resolution without involving the Court.

**B. *Native Files.***

1. Discoverable portions of electronic spreadsheets (*e.g.*, Excel), electronic presentations (*e.g.*, PowerPoint), desktop databases (*e.g.*, Access), and audio/video multimedia files shall be produced in native format as described in Paragraph A.13.a of Attachment A,

**C. *Enterprise Databases, Database Management Systems, and Other Structured Data (“Structured Data Systems”).***

1. If discoverable data from any Structured Data System can be produced in an already existing and reasonably available report, the Producing Party may collect and produce the data in that report format in accordance with Paragraph B.1.

2. If an existing report form is not reasonably available, the Producing Party may make reasonable efforts to export from the Structured Data System discoverable information in a format compatible with Microsoft Excel or Microsoft Access and may produce such information in that native format.

**D. *Use of Native Files in Proceedings in the Case.***

1. Unless the Parties agree otherwise in writing, a Party seeking to use a native file in any proceeding in this Action shall print a hardcopy (*i.e.*, paper copy) and shall mark that hardcopy as an exhibit. If printing a hardcopy is impracticable (*e.g.*, because of the excessive number of pages that would be required to be imaged or copied), the Party shall generate a hardcopy of at least five (5) pages that are representative of the entire native file. This provision shall not apply in the event of video proceedings, including those necessitated by the Covid-19 pandemic.

(a) When a TIFF image of the native file also was produced (*see* Paragraph II.A.1 above), the Party shall print the required hardcopy from that TIFF image.

(b) When the native file was initially produced in native format (*see* Paragraphs II.B and II.C.2 above), the Party seeking to use the native file shall:

- i. image the native file to TIFF image or PDF file in accordance with the specifications in Attachment A, Paragraphs A.3, A.4, and A.5;
- ii. include in the margin of each page of the TIFF image or PDF file (a) the original production number of the native file followed by a suffix indicating the page number from the native file, (b) the full confidentiality designation required by the Protective Order, and (c) the text, “file produced natively;”
- iii. prepend to the TIFF image or PDF file the associated slipsheet included with the initial production of the native file; and
- iv. print the required hardcopy from the resulting TIFF image or PDF file.



**2.** Prior to printing a hardcopy as set out in subparagraph D.1 immediately above, a Party may make alterations to a native file to facilitate its use with a witness or to use as an exhibit only on the following conditions:

**(a)** Such alterations shall not create a potential for confusion or prejudice.

i. On the condition that there be no confusion or prejudice, examples of permitted alterations include (a) hiding columns or rows that contain no information, and (b) hiding columns containing information not relevant to the columns presented and not otherwise reasonably relevant for context.

**(b)** The Party must make explicit and specific disclosure of each such alteration at a time at least 48 hours prior to use of the file in the proceeding.

**(c)** The Party seeking to use a hardcopy of an altered native file shall mark as exhibits both the hardcopy and a hardcopy of a slipsheet setting out (a) the information regarding the unaltered native file required by Attachment A, Paragraph 14.a, and (b) the MD5 or SHA-1 hash value of the originally produced unaltered native file.

**(d)** If a hardcopy prepared in accordance with these provisions is used at deposition, objections to its admissibility may be made within 60 days of its first use.

**3.** Reports Created from Native File Data.

**(a)** Subject to the limitations set out below, the parties are permitted to create from produced native files summaries, extracts, or reports to use as deposition exhibits. For example, a party may run a query over a large database extract to isolate data believed to be relevant and may create a

report from the same. Also by way of example, a party may extract information from native spreadsheets and create printouts of the same. Summaries, extracts, or reports must be accurate representations of the original data and are not authorized if they create a potential for confusion or prejudice.

- i. The party proposing to use a summary, extract, or report of a native file shall disclose in writing, at a time at least 48 hours prior to use of any such summary, extract, or report, a description of how it was created. As applicable, the description must identify the query run and the source data-set or must identify by Bates number the spreadsheet and the columns and rows extracted from it. The writing describing the methodology shall be marked as an exhibit.
- ii. If a summary, extract, or report prepared in accordance with these provisions is used at deposition, objections to its admissibility may be made within 60 days of its first use.

**4.** Nothing in this protocol waives the right of any Party to object on any grounds to use in any proceeding in this Action of a native file, of any altered native file, of any spreadsheet or TIFF-image associated with the native file, or of any summary, extract, or report of a native file.

**E. *Use of Search Filters.***

**1.** The Parties shall meet and confer to discuss the use of reasonable search filters such as word/phrase filters, proximity filters, or date filters, among other possible filters.

**(a)** The Producing Party will disclose its search terms to the Receiving Party to be applied to relevant ESI. If the Receiving Party believes, in good faith, the terms are deficient; the Parties will work collaboratively on

reaching agreement as to such filters, on the understanding that this may be an iterative process. Any proposed search filters shall be narrowly tailored to particular claims and defenses.

**(b)** Nothing in this order shall be deemed to be a waiver of any right or responsibility of the Producing Party to manage and control searches of its data files, including the right, upon notice to the Receiving Party, to make good-faith revisions to search filters.

**2.** The fact that any electronic file has been identified in agreed-upon searches shall not prevent any Party from withholding such file from production on the grounds that the file is not responsive, that it is protected from disclosure by applicable privilege or immunity, that it is governed by any applicable privacy law or regulation, that it contains commercially sensitive or proprietary non-responsive information, or that any protective order entered in this Action allows the file to be withheld.

**3.** Nothing in this section shall limit a Party's right reasonably to seek agreement from the other Parties or a court ruling to modify previously agreed-upon search filters.

**F. *Email Threading.***

**1.** Email threads are email communications that contain lesser-included email communications that also may exist separately in the Party's electronic document collection. A most-inclusive email is one that contains unique content and all the lesser-included emails, including attachments, for that branch of the email thread. The Parties agree that removal of available lesser-included emails from potential production will reduce all Parties' costs of document review, production, and litigation-support hosting, and, when producing the most-inclusive email in a thread, the parties need not also produce lesser-included emails in the thread.

**G.** Participants in lesser-included emails that otherwise would have been subject to review shall be listed in the most-inclusive email's "ALL\_PARTICIPANTS" field included in

the data load file (*see* Attachment A). Following production of the most inclusive email threads, for good cause and subject to the proportionality standard, a Receiving Party may make reasonable requests for individual lesser-included emails. The Producing Party shall cooperate reasonably in responding to any such requests if the requested lesser-included emails otherwise would have been subject to production.

**H. *Avoidance of Duplicate Production.***

1. “Duplicate ESI” means files that are exact duplicates based on the files’ MD5 or SHA-1 hash values. The Producing Party need produce only a single copy of responsive Duplicate ESI. A Producing party shall take reasonable steps to de-duplicate ESI globally (*i.e.*, both within a particular custodian’s files and across all custodians). Entire document families may constitute Duplicate ESI. De-duplication shall not break apart families. When the same Duplicate ESI exists in the files of multiple custodians, the additional custodians shall be listed in the CUSTODIANS field identified in Paragraph A.12(c) of Attachment A. Following the production of Documents, the Parties may meet and confer on any reasonable and proportional requests for information related to Duplicate ESI metadata, such as the file path information of Duplicate ESI that was not produced pursuant to this provision.

2. If the Producing Party makes supplemental productions following an initial production, that Party also shall provide with each supplemental production an overlay file to allow the Receiving Party to update the CUSTODIANS field. The overlay file shall include both all custodians listed in the CUSTODIANS field in prior productions and any custodians newly identified in the current supplemental production

**III. DOCUMENTS THAT EXIST ONLY IN HARDCOPY (PAPER) FORM**

A. A Party may produce documents that exist in the normal course of business only in hardcopy form either (a) in their original hardcopy form or (b) scanned and produced, redacted as necessary. The scanning of original hardcopy documents does not otherwise require that the scanned images be treated as ESI. The Parties will meet and confer on the scanning of any large

document sets (*i.e.* binders, file folders) into a single file if over 100 pages, to ensure they are being produced in a manner agreeable to the Parties. Nothing in this provision requires a Producing Party to employ coding of scanned documents to create family relationships during unitization.

#### **IV. CLAIMS OF PRIVILEGE**

**A.** Any document falling within the scope of any request for production or subpoena that is withheld on the basis of a claim of attorney-client privilege, work product, or any other claim of privilege or immunity from discovery is to be identified by the Producing Party in a separate privilege log twenty one (21) days after each production of documents for which a privilege is asserted. The Producing Party may utilize the procedures set forth in either IV.B or IV.C for the logging of privileged documents, at the Producing Party's discretion.

##### **B. Categorical Privilege Log**

- 1.** The parties may produce their privilege log in categorical format utilizing any reasoned method of organizing the documents that will facilitate an orderly assessment as to the appropriateness of withholding documents in the specified category. The parties shall identify the following for each category of documents:
  - (a)** The number of documents being withheld;
  - (b)** The date range for the withheld documents;
  - (c)** The senders and recipients of the documents including identification of attorneys and third-parties; and
  - (d)** The type(s) of privilege being asserted (*e.g.*, attorney-client, work product, joint defense, common interest, etc.); and
  - (e)** A description of the withheld documents, communication, or tangible things that, without revealing information claimed privileged or protected, will enable a party to assess the validity of efficacy of the privilege claim.
- 2.** The parties shall also produce a metadata log for all withheld documents with the following metadata fields (as described in ATTACHMENT A): CUSTODIANS, PAGES, AUTHOR, DATECREATED, DATELASTMOD, SUBJECT, FROM, TO, CC, BCC, DATESENT,

TIMESENT, DATERCVD, TIMERCVD. Additionally, parties shall assign control numbers for each document on the metadata log and provide a group identifier field for each document in order to associate document families together.

**C. Traditional Privilege Log**

1. For each document for which a Producing Party asserts that a privilege applies, the Producing Party must include in the privilege log the following information:
  - (a) a document identification number and/or Bates number;
  - (b) a statement of the ground(s) alleged for withholding such document;
  - (c) the date of the document or communication;
  - (d) the identity of its author and to whom it was sent (including To, From, CC and BCC);
  - (e) a description of the withheld document, communication, or tangible thing in a manner that, without revealing information claimed privileged or protected, will enable a party to assess the validity of efficacy of the privilege claim.

**D.** Notwithstanding a claim of privilege, except as otherwise set forth herein, any document containing both privileged and non-privileged matter must be produced with the purportedly privileged portion redacted, with the redacted portion indicated on the document itself. Such produced documents shall be accompanied by text files conforming to the specifications set out in Attachment A with only the redacted content removed. As set forth above, redacted documents do not need to be placed on a redaction or privilege log as long as the basis for the redaction is annotated on the redaction itself and the REDACTED and REDACTED TYPE metadata fields for the redacted documents are provided as set forth in attachment A. Following the production of redacted documents, a Receiving Party may make reasonable requests for privilege log entries related to individual documents redacted for privilege involving

in-house counsel or for redactions so substantial that they remove the context necessary to evaluate the asserted privilege, if there is a legitimate and good faith basis for questioning the privilege status of a document.

**E.** Privileged communications between a Party and their outside counsel or in-house counsel (to the extent that in-house counsel has acted solely in a legal rather than a business capacity) related to this Action or the facts that give rise to this Action do not need to be identified on a privilege log if those communications occurred on or after the filing of the complaint.

**F.** Following the receipt of a privilege log, a Receiving Party may identify, in writing, the particular documents that it believes require further explanation within thirty (30) days of receipt of the privilege log. Within thirty (30) days of such an identification, the Producing Party must respond to the request. If a Party challenges a request for further information, the Parties shall meet and confer to try to reach a mutually agreeable solution. If they cannot agree, the matter shall be brought to the Court.

**IT IS SO STIPULATED.**

Dated: March 23, 2021

/s/ Coty Montag  
Coty Montag  
Jennifer Holmes  
Jason Bailey  
NAACP Legal Defense and Education Fund, Inc.  
700 14th Street NW, Suite 600  
Washington, DC 20005  
Telephone: 202-216-5573  
Facsimile: 202-682-1312  
E-mail: cmontag@naacpldf.org  
jholmes@naacpldf.org  
jbailey@naacpldf.org

Rebecca A. Maurer (0095401)  
MAURER LAW LLC  
6815 Euclid Avenue  
Cleveland, Ohio 44103  
Telephone: 216-242-6672  
Facsimile: 216-242-6691  
E-mail: rebecca@maurerlawllc.com

Neil K. Roman  
Henry Liu  
Margaret H. Brennan  
Cyril Djoukeng  
COVINGTON & BURLING LLP  
One CityCenter  
850 Tenth Street, NW  
Washington, DC 20001  
Tel: (202)-662-6000  
Email: nroman@cov.com  
hliu@cov.com  
mbrennan@cov.com  
cdjoukeng@cov.com

*Attorneys for Plaintiffs*

Dated: March 23, 2021

/s/ Robert J. Hanna  
Robert J. Hanna (0037230)  
Sanford E. Watson (0040862)  
Michael J. Ruttinger (0083850)  
Christine M. Snyder (0086788)  
Tucker Ellis LLP  
950 Main Avenue, Suite 1100  
Cleveland, OH 44113-7213  
Telephone: 216.592.5000  
Facsimile: 216.592.5009  
E-mail: robert.hanna@tuckerellis.com  
sanford.watson@tuckerellis.com  
michael.ruttinger@tuckerellis.com  
christine.snyder@tuckerellis.com

Barbara A. Langhenry (0038838)  
Director of Law  
City of Cleveland, Ohio  
Department of Law  
601 Lakeside Avenue, Room 106  
Cleveland, OH 44114-1077  
Telephone: 216.664.2800



Facsimile: 216.420.8560  
E-mail: blanghenry@city.cleveland.oh.us

*Attorneys for Defendant City of Cleveland*

**ATTACHMENT A**

A.1. **Image Files.** Files produced in .tiff format will be single page black and white .tiff images at 300 DPI, Group IV compression. To the extent possible, original orientation will be maintained (*i.e.*, portrait-to-portrait and landscape-to-landscape). Each .tiff image will be assigned a unique name matching the production number of the corresponding page. Such files will be grouped in folders of no more than 2,500 .tiff files each unless necessary to prevent a file from splitting across folders. If a file, *e.g.*, a PDF file, exceeds 500 .tiff images, the producing party may produce the file natively rather than in .tiff format. Files will not be split across folders and separate folders will not be created for each file. Production (“Bates”) numbers shall be endorsed on the lower right corner of all images. This number shall be a unique, consistently formatted identifier that will:

- a. be consistent across the production;
- b. contain no special characters; and
- c. be numerically sequential within a given file.

Bates numbers should be a combination of an alpha prefix along with an 8-digit number (*e.g.*, ABC00000001). The number of digits in the numeric portion of the Bates number format should not change in subsequent productions. Confidentiality designations, if any, will be endorsed on the lower left or right corner of all images and shall not obscure any portion of the original file.

A.2. **File Text.** The production of any ESI containing extractable text shall be accompanied by full text as file (not page) level files formatted as UTF-8 text files with the text file named to match the beginning production number of the file. The full path of the text file must be provided in the .dat data load file. Where ESI has been redacted to remove privileged

or protected content, the ESI shall be produced with text files conforming to the above with only the redacted content removed.

- A.3. **Word Processing Files.** If word processing files, including without limitation Microsoft Word files (.doc and .docx), are produced in .tiff image format, such .tiff images will display tracked changes, comments, and hidden text, to the extent available.
- A.4. **Presentation Files.** If presentation files, including without limitation Microsoft PowerPoint files (.ppt and .pptx), are produced in .tiff image format, such .tiff images will display comments, hidden slides, speakers' notes, and similar data in such files.
- A.5. **Spreadsheet or Worksheet Files.** If spreadsheet files, including without limitation Microsoft Excel files (.xls or .xlsx), are produced in .tiff image format, such .tiff images will display hidden rows, columns, and worksheets, if any, in such files.
- A.6. **Parent-Child Relationships.** Parent-child relationships (*e.g.*, the associations between emails and their attachments) will be preserved. Email and other ESI attachments will be produced as independent files immediately following the parent email or ESI record. Parent-child relationships will be identified in the data load file pursuant to paragraph A.12 below.
- A.7. **English Language.** To the extent any data exists in more than one language, the data will be produced in English, if available. If no English version of a file is available, the Producing Party shall not have an obligation to produce an English translation of the data.
- A.8. **Embedded Objects.** Some files ("containing files") may contain embedded objects. Such objects typically are the following file types: Microsoft Excel, Word, PowerPoint, Project, Outlook, and Access; and PDF. Subject to applicable claims of privilege or immunity, embedded objects with those identified file types shall be extracted as separate files, if reasonably feasible technologically, and shall be produced as attachments to the containing file, unless the containing file is produced in native format, because, in that case, the embedded objects are produced as part of the native containing file, unless the

embedded object is fully contained in the production images (*e.g.*, an embedded table whose data is fully displayed in the produced image).

A.9. **Compressed Files.** Compressed file types (*i.e.*, .CAB, .GZ, .TAR, .Z, .ZIP) shall be decompressed in a reiterative manner to ensure that a zip within a zip is decompressed into the lowest possible compression resulting in individual files.

A.10. **Scanned Hardcopy Documents.**

For scanned images of hard copy documents, OCR should be performed on a document level and provided in document-level .txt files named to match the production number of the first page of the document to which the OCR text corresponds similar to other ESI.

A.11. **Production Numbering.**

In following the requirements of Paragraph A.1, the Producing Party shall take reasonable steps to ensure that attachments to documents or electronic files are assigned production numbers that directly follow the production numbers on the documents or files to which they were attached. If a production number or set of production numbers is skipped, the skipped number or set of numbers will be noted. In addition, each .tiff image will have its assigned production number electronically “burned” onto the image.

A.12. **Data and Image Load Files.**

a. Load Files Required. Unless otherwise agreed, each production will include a data load file in Concordance (.dat) format and an image load file in Opticon (.opt) format.

b. Load File Formats.

i. Load file names should contain the volume name of the production media. Additional descriptive information may be provided after the volume name. For example, both ABC001.dat or ABC001\_metadata.dat would be acceptable.

- ii. Unless other delimiters are specified, any fielded data provided in a load file should use Concordance default delimiters. Semicolon (;) should be used as multi-entry separator.
  - iii. Any delimited text file containing fielded data should contain in the first line a list of the fields provided in the order in which they are organized in the file.
- c. Fields to be Included in Data Load File. For all documents or electronic files identified as relevant, not privileged, and produced, the following metadata fields for each document or electronic file, if available at the time of collection and processing and unless such metadata fields are protected from disclosure by attorney-client privilege or work-product immunity or otherwise prohibited from disclosure by law or regulation, will be provided in the data load file pursuant to subparagraph (a). The term “Scanned Docs” refers to documents that are in hard copy form at the time of collection and have been scanned into .tiff images OR PDFs. The term “Email and E-Docs” refers to files that are in electronic form at the time of their collection, irrespective of the form (TIFF or native format) in which they are produced.

Field	Sample Data	Scanned Docs	Email and E-Docs	Comment
PRODBEG [Key Value]	ABC00000001	Yes	Yes	Beginning production number
PRODEND	ABC00000008	Yes	Yes	Ending production number
PRODBEGATT	ABC00000009	N/A	Yes	Beginning production number of parent in a family

Field	Sample Data	Scanned Docs	Email and E-Docs	Comment
PRODENDATT	ABC00001005	N/A	Yes	Ending production number of last page of the last attachment in a family
CUSTODIANS	Smith, John	Yes	Yes	All custodians who possessed the document or electronic file; when global de-duplication is used, this includes custodians whose file has been de-duplicated; multiple custodians separated by semicolons
NATIVEFILE	Natives\001\001\ABC00000001.xls	N/A	Yes	Path and file name for native file on production media
FILEPATHS	C:\Users\JaneDoe\Documents\Document1.doc	N/A	Yes	Original source file path for the record produced (in other words, the location where the file was collected);
FILENAME	Document1.doc	N/A	Yes	Name of original electronic file as collected.
DOEXT	DOC	N/A	Yes	File extension for email or e-doc
PAGES	2	Yes	Yes	Number of pages in the produced document or electronic file (not applicable to native file productions).
AUTHOR	John Smith	N/A	Yes	Author information as derived from the properties of the document.
DATECREATED	10/09/2005	N/A	Yes	Date on which non-email file was created as extracted from file system metadata

Field	Sample Data	Scanned Docs	Email and E-Docs	Comment
DATELASTMOD	10/09/2005	N/A	Yes	Last date on which non-email file was modified as extracted from file system metadata
SUBJECT	Changes to Access Database	N/A	Yes	“Subject” field extracted from email message or metadata properties of the document
FROM	John Beech	N/A	Yes	“From” field extracted from email message
TO	Janice Birch	N/A	Yes	“To” field extracted from email message
CC	Frank Maple	N/A	Yes	“Cc” or “carbon copy” field extracted from email message
BCC	John Oakwood	N/A	Yes	“Bcc” or “blind carbon copy” field extracted from email message
DATESENT	10/10/2005	N/A	Yes	Sent date of email message (mm/dd/yyyy format)
TIMESENT	10:33 am	N/A	Yes	Sent time of email message, time zone set to GMT
DATERCVD	10/10/2005	N/A	Yes	Received date of email message (mm/dd/yyyy format)
TIMERCVD	10:33 am	N/A	Yes	Received time of email message, time zone set to GMT
ALL_PARTICIPANTS	John Beech; Janice Birch; Frank Maple	N/A	Yes	For emails only; lists all participants, in a delimited list, in lesser-included emails that, without threading, would have been subject to review

Field	Sample Data	Scanned Docs	Email and E-Docs	Comment
CONFIDENTIALITY	HIGHLY CONFIDENTIAL	Yes	Yes	Text of confidentiality designation(s), if any
TEXTPATH	Text\001\001\ABC00000001.txt	Yes	Yes	Path to .txt file containing extracted or OCR text
NATIVEPATH	Native\001\001\ABC00000001.xls	N/A	Yes	Path to Native file in the production
MD5_HASH	309997447f.....	N/A	Yes	MD5 Hash value for ESI
PRODVOL	VOL001	Yes	Yes	Name of the Production Volume
REDACTED	Yes	Yes	Yes	Identifies whether a Document contains redactions
REDACTED TYPE	Privilege	Yes	Yes	Identifies the reason for a redaction

#### A.13. Files Produced in Native Format.

- a. For any electronic file produced initially as a native file in accordance with Paragraph II.B of the Protocol above, the file shall be given a file name consisting of a unique Bates number and, as applicable, a suitable confidentiality designation; for example, “ABC00000002\_Confidential.” For each such native file, the production will include a .tiff image slipsheet (i) indicating the production number of the native file, (ii) with respect to any confidential document, setting forth the full confidentiality language applicable to the native file as set out in the protective order, and (iii) stating “File Provided Natively.” To the extent that it is available, the original or redacted file text shall be provided in a file-level multi-page UTF-8 text file with a text path provided in the .dat file; otherwise the text contained on the slipsheet shall be provided in the .txt file with the text path provided in the .dat file.

- b. For any electronic file produced in native file format following production of a TIFF-image in accordance with Paragraph II.A, the file shall be given a file name consisting of (i) the Bates number of the first page of the associated TIFF-image and (ii) as applicable, a suitable confidentiality designation. For each such native file, the production will include a new .DAT file (i) indicating the production number of the native file, (ii) identifying the path to the native file, (iii) adding a field stating “Yes,” indicating that the file was produced in both native and TIFF formats, and (iv) linking the metadata associated with the originally produced TIFF image to the newly produced native file.
- A.14. **Production Media.** Unless otherwise agreed, documents and ESI will be produced on encrypted USB drive, encrypted external hard drive, secure FTP site, or similar electronic format. Such media should have an alphanumeric volume name; if a hard drive contains multiple volumes, each volume should be contained in an appropriately named folder at the root of the drive. Volumes should be numbered consecutively (ABC001, ABC002, etc.). Deliverable media should be labeled with the name of this action, the identity of the producing Party, and the following information: Volume name, production range(s), and date sent.
- A.15. **Encryption of Production Media.** To maximize the security of information in transit, any media on which documents or electronic files are produced shall be encrypted by the producing Party. The producing Party shall transmit the encryption key or password to the requesting Party, under separate cover, contemporaneously with sending the encrypted media.